IN THE UNITED STATES PATENT AND TRADEMARK OFFICE





**Applicants:** Satoshi Hada

**Serial No.:** 09/819,359

**Filed:** March 28, 2001

**For:** USER AUTHENTICATION METHOD, AND STORAGE MEDIUM, APPARATUS AND SYSTEM THEREFOR

**Examiner**: Piotr Poltorak

**Art Unit:** 2134

**Docket:** JP919990280US1 (18418)

**Dated:** March 21, 2005

**Confirmation No:** 3306

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## CLAIM OF PRIORITY

Sir:

Applicant in the above-identified application hereby claim the right of priority in connection with Title 35 U.S.C. §119 and in support thereof, herewith submit a certified copy of Japanese Patent Application No. 2000-099867 filed on March 31, 2000.

Respectfully submitted,

Steven Fischman
Registration No. 34,594

Scully, Scott, Murphy & Presser
400 Garden City Plaza, Suite 300
Garden City, NY 11530
(516) 742-4343
SF:gc

---

## CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, P.O. Box 1450, Alexandria, VA 22313-1450 on March 21, 2005.

Dated: March 21, 2005

Steven Fischman

# 日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出願年月日
Date of Application: ２０００年　３月３１日

出願番号
Application Number: 特願２０００－０９９８６７

願人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレーション





２０００年　９月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０７４７６８

【書類名】　特許願

【整理番号】　JA999280

【提出日】　平成12年 3月31日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　1/00

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　羽田　知史

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレイション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【復代理人】

【識別番号】　100079049

【弁理士】

【氏名又は名称】　中島　淳

【電話番号】　03-3357-5171

【選任した復代理人】

【識別番号】　100084995

【弁理士】

【氏名又は名称】　加藤　和詳

【電話番号】　03-3357-5171

【選任した復代理人】

【識別番号】　100085279

【弁理士】

【氏名又は名称】　西元　勝一

【電話番号】　03-3357-5171

【選任した復代理人】

【識別番号】　100099025

【弁理士】

【氏名又は名称】　福田　浩志

【電話番号】　03-3357-5171

【手数料の表示】

【予納台帳番号】　006839

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9304391

【包括委任状番号】　9304392

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　ユーザ認証方法、記憶媒体、装置及びシステム

【特許請求の範囲】

【請求項１】　証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証方法であって、

前記証明者側装置は乱数ａを生成し、暗号Ａ＝関数Ｆ（ｇ，ａ）を求め、該暗号Ａを検証者側装置に送信し、

前記検証者側装置は乱数ｂを生成し、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求め、該暗号Ｂ，Ｘを証明者側装置に送信し、

前記証明者側装置は、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証し、成立すると検証したときに、乱数ｃを生成し、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求め、該各暗号を検証者側装置に送信し、

前記検証者側装置は暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証する

ことを特徴とするユーザ認証方法。

【請求項２】　（ｑ｜ｐ－１）の関係を満たす素数ｐ，ｑと、位数ｑの元を前記整数ｇとして、公開鍵ｖを求めることを特徴とすることを特徴とする請求項１のユーザ認証方法。

【請求項３】　前記関数Ｆは、前記公開鍵ｖと秘密鍵ｓを用いて

$v = F(g, -s) = g^{-s} \bmod p$

の関係を有することを特徴とすることを特徴とする請求項１のユーザ認証方法。

【請求項４】　前記証明者側装置は、

$X = B^{a} \bmod p$

の関係が成立したときに乱数ｃを生成することを特徴とすることを特徴とする請求項１のユーザ認証方法。

【請求項５】　前記関数Ｈは、

Ｈ（ａ，Ｙ，ｓ）＝ａ＋Ｙｓ　ｍｏｄ　ｑ

の関係を有することを特徴とすることを特徴とする請求項１のユーザ認証方法。

【請求項６】　前記関数Ｊは、

$J(v, Y, g, Z) = v^{Y} g^{Z} \bmod p$

の関係を有することを特徴とすることを特徴とする請求項１のユーザ認証方法。

【請求項７】　証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための証明者側装置用プログラムを記録した前記証明者側装置において読み取り可能な記録媒体であって、前記証明者側装置に、

乱数ａを生成させ、暗号Ａ＝関数Ｆ（ｇ，ａ）を求めさせ、該暗号Ａを検証者側装置に送信させ、

前記検証者側装置からの暗号Ｂ，Ｘを受信させ、

受信された暗号Ｂ，Ｘに基づいて、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証させ、成立すると検証されたときに、乱数ｃを生成させ、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求めさせ、該各暗号を検証者側装置に送信させる

証明者側装置用プログラムを記録した記録媒体。

【請求項８】　証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための検証者側装置用プログラムを記録した前記検証者側装置において読み取り可能な記録媒体であって、前記検証者側装置に、

前記証明者側装置からの暗号Ａを受信させ、

乱数ｂを生成させ、該乱数ｂおよび受信された暗号Ａに基づいて、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求め、該暗号Ｂ，Ｘを証明者側装置に送信させ、

前記証明者側装置からの暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを受信させ、

受信された暗号Ｃ、Ｙ、Ｚに基づいて、暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証させる

検証者側装置用プログラムを記録した記録媒体。

【請求項９】　証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための証明者側装置用のユーザ認証装置において、

乱数ａを生成しかつ暗号Ａ＝関数Ｆ（ｇ，ａ）を求め、求めた暗号Ａを検証者側装置に送信する送信手段と、

前記検証者側装置からの暗号Ｂ，Ｘを受信する受信手段と、

受信された暗号Ｂ，Ｘに基づいて、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証する検証手段と、

前記成立すると検証されたときに、乱数ｃを生成しかつ、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求める暗号演算手段と、

前記暗号Ｃ，Ｙ，Ｚを検証者側装置に送信する暗号送信手段と、

を備えたことを特徴とする証明者側装置用のユーザ認証装置。

【請求項１０】　証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定めら

れ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための検証者側装置用のユーザ認証装置において、

前記証明者側装置からの暗号Ａを受信する受信手段と、

乱数ｂを生成しかつ、該乱数ｂおよび受信された暗号Ａに基づいて、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求めて、該暗号Ｂ，Ｘを証明者側装置に送信する送信手段と、

前記証明者側装置からの暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを受信する暗号受信手段と、

受信された暗号Ｃ、Ｙ、Ｚに基づいて、暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証する検証手段と、

を備えたことを特徴とする検証者側装置用のユーザ認証装置。

【請求項１１】　請求項９に記載の証明者側装置用のユーザ認証装置と、

複数の請求項１０に記載の検証者側装置用のユーザ認証装置と、

を含むユーザ認証システム。

【請求項１２】　証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証システムにおいて、

乱数ａを生成しかつ暗号Ａ＝関数Ｆ（ｇ，ａ）を求め、求めた暗号Ａを検証者側装置に送信する証明者側装置用送信手段と、

前記証明者側装置からの暗号Ａを受信する検証者側装置用受信手段と、

乱数ｂを生成し、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求め、該暗号Ｂ，Ｘを証明者側装置に送信する検証者側装置用送信手段と、

前記検証者側装置からの暗号Ｂ，Ｘを受信する証明者側装置用受信手段と、

受信された暗号Ｂ，Ｘに基づいて、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証する証明者側装置用検証手段と、

前記成立すると検証されたときに、乱数ｃを生成しかつ、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求める証明者側装置用暗号演算手段と、

前記暗号Ｃ，Ｙ，Ｚを検証者側装置に送信する証明者側装置用暗号送信手段と、

前記証明者側装置からの暗号Ｃ，Ｙ，Ｚを受信する検証者側装置用暗号受信手段と、

暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証する検証者側装置用検証手段と、

を含むことを特徴とするユーザ認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに接続されたコンピュータシステム等の装置におけるユーザ認証方法、ユーザ認証プログラムを記憶した記憶媒体、ユーザ認証装置及びユーザ認証システムにかかり、特に、少なくとも公開鍵が設定された証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証方法、ユーザ認証プログラムを記憶した記憶媒体、ユーザ認証装置及びユーザ認証システムに関する。

【０００２】

【従来の技術】

ネットワーク上において、あるユーザが自分の身元を証明するためには、ユーザ認証が必要である。ユーザ認証とは、何らかのプロトコルにより、証明者が自分の身元を検証者に対して証明することであり、電子商取引などの分野において、必須の技術である。例えば、ユーザがサーバに対して、身元を証明したいときは、ユーザが証明者に、サーバが検証者に対応する。また、逆に、サーバがユーザに対して身元を証明したい場合は、サーバが証明者に、ユーザが検証者に対応

する。ユーザ認証は、ユーザとサーバの間に限定されず、任意のコンピュータ間での身元を証明する方法として、幅広く利用されている。最近のユーザ認証では、公開鍵暗号に基づいており、証明者は公開鍵と秘密鍵を所持しており、証明者が公開鍵に対応する秘密鍵を所持することを、なんらかのプロトコルにより、検証者に示すことにより、身元を証明している。

【０００３】

このユーザ認証の代表的な技術として、Schnorrの方法が知られている（C. P. Schnorr, "EfficientSignature Generation by Smart Cards,"Journal of Cryptology, Vol.4, No.3,pp.161-174, 1991.参照）。この技術では、証明者は検証者に対して、公開鍵に対応する秘密鍵を所持することを証明することにより、ユーザ認証を実現している。

【０００４】

従来の技術の一例として、このSchnorrのユーザ認証方法についてその概要を図３を参照して説明する。この方法で用いるシステム・パラメータは、素数ｐ、ｑ（但し、ｑ｜ｐ－１）と、位数ｑの元ｇ∈Ｚｐである。また、証明者の公開鍵は、ｖ（但し、$v = g^{-s} \bmod p$）である。証明者の秘密鍵は、ｓ∈Ｚｑである。なお、以下の説明では、証明者及び検証者は、システム・パラメータである素数ｐ、ｑ、及び元ｇも予め取得しているものとし、検証者は証明者の公開鍵ｖを予め取得しているものとする。

【０００５】

この方法における検証者と証明者の情報授受は次の通りである。

ステップ１　証明者は乱数ａ∈Ｚｑを生成し、

$A = g^{a} \bmod p$

を計算し、検証者に送信する。

ステップ２　検証者は乱数ｂ（ｂ∈Ｚｑ）を生成し、

証明者に送信する。

ステップ３　証明者は

$c = a + bs \bmod q$

を計算し、検証者に送信する。

ステップ４　検証者は、

$$A = v^{b} g^{c} \bmod p$$

が成立するかどうかを検証し、成立すれば証明者は正当であるとみなす。一方、不成立の場合には、証明者の身元が不当であるとみなし、拒否する。

【０００６】

このSchnorrの方法は、離散対数問題に基づく方法の中で、最も効率的である。特に、その通信回数は３回である。しかしながら、その安全性は証明されていない。すなわち、ネットワーク上で、プロトコルが実行される過程で、証明者の秘密鍵ｓが露呈する可能性を含んでいる。そこで、証明者と検証者との間の情報授受すなわちユーザ認証（メッセージのを送受信等）に対して安全性を評価することが考えられるが、この評価すなわちユーザ認証の安全性について、零知識性に関する技術がよく知られている（S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proofs," Proceedings of 17th synposium on Theory of Computing, pp.291-304, 1985. 参照）。零知識性は、証明者の秘密鍵に関する情報が、一切露呈しないことを意味するものであり、零知識性を満たすことでユーザ認証方法の安全性が保証される。

【０００７】

上記のSchnorrの認証方法では、一部を修正することで零知識性を有することになる（A. Fiat and A.Shamir, "How to prove yourself: practical solution to identification and signature problems," Proceedings of Crypto'86, 1980.参照）。具体的には、検証者による乱数をｂ∈｛０，１｝として生成し、プロトコルを０（ｌｏｇ　ｑ）回、シーケンシャルに実行するように修正すれば、零知識性を満たすことが証明されている。すなわち、以下のプロトコルを０（ｌｏｇ　ｑ）回実行し、全ての実行において、検証者が受理するならば、最終的に証明者の身元を認証するものである。

【０００８】

〔プロトコル〕

ステップ１：証明者は、乱数　ａ∈Ｚｑを生成し、

$A = g^a \bmod p$

を計算し、Ａを検証者に送信する。

ステップ２　検証者は乱数ｂ∈｛０，１｝を生成し、

証明者に送信する。

ステップ３　証明者は

$c = a + bs \bmod q$

を計算し、ｃを検証者に送信する。

ステップ４　検証者は、

$A = v^b g^c \bmod p$

が成立するかどうかを検証し、成立すれば証明者は正当であるとみなす。一方、不成立の場合には、証明者の身元が不当であるとみなし、拒否する。

【０００９】

このように、通信回数は０（ｌｏｇ　ｑ）に増加するが、零知識性は保証される。上記のSchnorrの認証方法以外にも、零知識性を満たすユーザ認証方法は、従来から数多く知られている。

【００１０】

【発明が解決しようとする課題】

しかしながら、従来のユーザ認証方法における零知識性は、証明者と検証者とが１対１であることを前提としており、証明者と検証者との間が１対１でプロトコルを実行するときのみに満たされる（図４参照）。すなわち、証明者が複数の検証者と同時にプロトコルを実行する必要がある場合、零知識性が満たされる保証はない（C. Dwork, M. Naor and A. Sahai, "Concurrent Zero-Knowledge, " Proc. Of $30^{th}$ STOC, 1998. 参照）。

【００１１】

例えば、インターネットのような非同期型ネットワークでは、複数のコンピュータが同時に通信しており、証明者が複数の検証者と同時にプロトコルを実行する場合がある。WWW（World Wide Web:ワールド・ワイド・ウェブ）では、ＨＴＴＰ（Hypertext Transfer Protocol :WWWサーバーとWWWブラウザやWebブラウ

ザ等が、ファイル等の情報授受に使うプロトコル）のサーバは、接続先である複数のクライアントに対して同時に、自分の身元を証明することが要求される（図５参照）。

【００１２】

本発明は、上記事実を考慮して、証明者と検証者が多数の場合であっても零知識性を満たしながら安全にユーザ認証することができるユーザ認証方法、ユーザ認証プログラムを記憶した記憶媒体、ユーザ認証装置及びユーザ認証システムを得ることが目的である。

【００１３】

【課題を解決するための手段】

上記目的を達成するために本発明は、証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証方法であって、前記証明者側装置は乱数ａを生成し、暗号Ａ＝関数Ｆ（ｇ，ａ）を求め、該暗号Ａを検証者側装置に送信し、前記検証者側装置は乱数ｂを生成し、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求め、該暗号Ｂ，Ｘを証明者側装置に送信し、前記証明者側装置は、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証し、成立すると検証したときに、乱数ｃを生成し、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求め、該各暗号を検証者側装置に送信し、前記検証者側装置は暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証することを特徴とする。

【００１４】

（ｑ｜ｐ－１）の関係を満たす素数ｐ，ｑと、位数ｑの元を前記整数ｇとして、公開鍵ｖを求めることを特徴とすることを特徴とする。

【００１５】

前記関数Ｆは、前記公開鍵ｖと秘密鍵ｓを用いて

$v = F(g, -s) = g^{-s} \bmod p$

の関係を有することを特徴とする。

【００１６】

前記証明者側装置は、

$X = B^{a} \bmod p$

の関係が成立したときに乱数ｃを生成することを特徴とする。

前記関数Ｈは、

$H(a, Y, s) = a + Ys \bmod q$

の関係を有することを特徴とする。

前記関数Ｊは、

$J(v, Y, g, Z) = v^{Y} g^{Z} \bmod p$

の関係を有することを特徴とする。

【００１７】

また、他の発明は、証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための証明者側装置用プログラムを記録した前記証明者側装置において読み取り可能な記録媒体であって、前記証明者側装置に、乱数ａを生成させ、暗号Ａ＝関数Ｆ（ｇ，ａ）を求めさせ、該暗号Ａを検証者側装置に送信させ、前記検証者側装置からの暗号Ｂ，Ｘを受信させ、受信された暗号Ｂ，Ｘに基づいて、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証させ、成立すると検証されたときに、乱数ｃを生成させ、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求めさせ、該各暗号を検証者側装置に送信させる。

【００１８】

また、他の発明は、証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の

関係についての正当性を検証するユーザ認証のための検証者側装置用プログラムを記録した前記検証者側装置において読み取り可能な記録媒体であって、前記検証者側装置に、前記証明者側装置からの暗号Ａを受信させ、乱数ｂを生成させ、該乱数ｂおよび受信された暗号Ａに基づいて、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求め、該暗号Ｂ，Ｘを証明者側装置に送信させ、前記証明者側装置からの暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを受信させ、受信された暗号Ｃ、Ｙ、Ｚに基づいて、暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証させる。

【００１９】

また、他の発明は、証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための証明者側装置用のユーザ認証装置において、乱数ａを生成しかつ暗号Ａ＝関数Ｆ（ｇ，ａ）を求め、求めた暗号Ａを検証者側装置に送信する送信手段と、前記検証者側装置からの暗号Ｂ，Ｘを受信する受信手段と、受信された暗号Ｂ，Ｘに基づいて、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証する検証手段と、前記成立すると検証されたときに、乱数ｃを生成しかつ、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求める暗号演算手段と、前記暗号Ｃ，Ｙ，Ｚを検証者側装置に送信する暗号送信手段と、を備えたことを特徴とする。

【００２０】

また、他の発明は、証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証のための検証者側装置用のユーザ認

証装置において、前記証明者側装置からの暗号Ａを受信する受信手段と、乱数ｂを生成しかつ、該乱数ｂおよび受信された暗号Ａに基づいて、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求めて、該暗号Ｂ，Ｘを証明者側装置に送信する送信手段と、前記証明者側装置からの暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを受信する暗号受信手段と、受信された暗号Ｃ、Ｙ、Ｚに基づいて、暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証する検証手段と、を備えたことを特徴とする。

【００２１】

また、他の発明のユーザ認証システムは、前記証明者側装置用のユーザ認証装置と、複数の前記検証者側装置用のユーザ認証装置と、を含んでいる。

【００２２】

また、他の発明のユーザ認証システムは、証明者側装置の公開鍵ｖと秘密鍵ｓとの関係について予め定めた整数ｇを用い、ｖ＝Ｆ（ｇ，－ｓ）を満たすべき一方向性関数Ｆが定められ、証明者側装置と複数の検証者側装置との間で証明者側装置と検証者側装置の関係についての正当性を検証するユーザ認証システムにおいて、乱数ａを生成しかつ暗号Ａ＝関数Ｆ（ｇ，ａ）を求め、求めた暗号Ａを検証者側装置に送信する証明者側装置用送信手段と、前記証明者側装置からの暗号Ａを受信する検証者側装置用受信手段と、乱数ｂを生成し、暗号Ｂ＝関数Ｆ（ｇ，ｂ）と暗号Ｘ＝関数Ｆ（Ａ，ｂ）を求め、該暗号Ｂ，Ｘを証明者側装置に送信する検証者側装置用送信手段と、前記検証者側装置からの暗号Ｂ，Ｘを受信する証明者側装置用受信手段と、受信された暗号Ｂ，Ｘに基づいて、暗号Ｘ＝関数Ｆ（Ｂ，ａ）の関係の成立性を検証する証明者側装置用検証手段と、前記成立すると検証されたときに、乱数ｃを生成しかつ、暗号Ｃ＝関数Ｆ（ｇ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｂ，ｃ）と、または暗号Ｃ＝関数Ｆ（Ａ，ｃ）及び暗号Ｙ＝関数Ｆ（Ｘ，ｃ）と、暗号Ｚ＝関数Ｈ（ａ，Ｙ，ｓ）とを求める証明者側装置用暗号演算手段と、前記暗号Ｃ，Ｙ，Ｚを検証者側装置に送信する証明者側装置用暗号送

信手段と、前記証明者側装置からの暗号Ｃ，Ｙ，Ｚを受信する検証者側装置用暗号受信手段と、暗号Ｙ＝関数Ｆ（Ｃ，ｂ）及び暗号Ａ＝関数Ｊ（ｖ，Ｙ，ｇ，Ｚ）の２つの関係が同時に成立したときに、前記検証者側装置と前記証明者側装置の関係が正当であると検証する検証者側装置用検証手段と、を含むことを特徴とする。

【００２３】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態の一例を詳細に説明する。本実施の形態は、ネットワークにおいて公開鍵ｖと秘密鍵ｓを用いてユーザ認証する場合に本発明を適用したものである。

【００２４】

本発明は、インターネットなどの非同期ネットワークにおいてユーザ認証するためのものである。非同期なネットワークでは、証明者が、複数の検証者に対して、同時に、ユーザ認証のプロトコルを実行されることを要求される可能性がある。つまり、本実施の形態では、１つの証明者に対して、複数の検証者が存在することを想定している。

【００２５】

本実施の形態では、暗号化するための関数として次に示す一方向性関数Ｆを用いている。一方向性関数Ｆは、２入力、１出力の関数であり、２番目の変域と値域では、それぞれにおいて、加算（＋）と乗算（＊）の二つの演算が定義されているものとする。

さらに、関数Ｆは、次の２つの性質を満たす。

すなわち、任意のａ，ｂに関して、

① Ｆ（ｇ，ａ＋ｂ）＝Ｆ（ｇ，ａ）＊Ｆ（ｇ，ｂ）

② Ａ＝Ｆ（ｇ，ａ）ならば、Ｆ（ｇ，ａ＊ｂ）＝Ｆ（Ａ，ｂ）

の両方が成り立たなければならない。

また、他の暗号化のための関数Ｈは、次のように表される。関数Ｈは、３入力、１出力の関数である。

Ｈ（ａ，Ｙ，ｓ）＝ａ＋Ｙ＊ｓ

ただし、ここでの加算と乗算は、関数Ｆの２番目の変域で定義されるものである。

さらに、他の暗号化のための関数Ｊは、４入力、１出力の関数であるが関数Ｆにより、次のように表される。

Ｊ（ｖ，Ｙ，ｇ，Ｚ）＝Ｆ（ｖ，Ｙ）＊Ｆ（ｇ，Ｚ）

と表される。

【００２６】

関数Ｆの具体例として、離散対数問題に基づく一方向性関数が考えられる。その代表的な例は、素数ｐ，ｑがｑ｜ｐ－１の関係を有し、ｇ∈Ｚｐが位数ｑの元であるとしたとき、

$F(g, a) = g^a \bmod p$

である。

【００２７】

まず、本発明が適用可能な装置を図２に示した。ネットワーク３２には、各々ＣＰＵを少なくとも含むコンピュータにより構成された証明者側装置１０、検証者側装置４０、及び検証者側装置４０と同様の構成である他の検証者側装置６０が複数接続されている。このように、本実施の形態では、証明者側装置と、検証者側装置とが１対多の接続関係になっている。

【００２８】

証明者側装置１０は、システムパラメータ等を入力するための入力装置１２を備えており、入力装置１２は入力に応じた乱数ａを発生する乱数発生器１４及びメモリ１６に接続されている。乱数発生器１４は、メモリ１６及び乱数ａに基づく暗号Ａを求める暗号演算器１８に接続されている。暗号演算器１８は、ネットワーク３２を介して他の装置と通信するためにネットワーク３２に接続された通信インタフェース（以下、通信Ｉ／Ｆという）３０に接続されている。通信Ｉ／Ｆ３０には、検証器２０が接続されている。この検証器２０はメモリ１６も接続されている。また、検証器２０は、入力に応じた乱数ｃを発生する乱数発生器２２及び入力信号により後述するプロトコルを中断する中断装置２４に接続されている。乱数発生器２２は、乱数ｃに基づく暗号Ｃ，Ｙを求める暗号演算器２６に

接続され、暗号演算器２６は暗号Ｃ，Ｙに基づく暗号Ｚを求める暗号演算器２８に接続されている。また、暗号演算器２６、２８は、通信Ｉ／Ｆ３０に接続されると共に、メモリ１６にも接続されている。

【００２９】

検証者側装置４０は、システムパラメータ等を入力するための入力装置４２を備えており、入力装置４２は入力に応じた乱数ｂを発生する乱数発生器４４及びメモリ４６に接続されている。乱数発生器４４は、メモリ４６及び乱数ｂに基づく暗号Ｂ，Ｘを求める暗号演算器４８に接続されている。暗号演算器１８は、ネットワーク３２を介して他の装置と通信するために通信Ｉ／Ｆ５６に接続されている。通信Ｉ／Ｆ５６には、検証器５０が接続されている。この検証器５０はメモリ４６も接続されている。また、検証器２０は、その出力側に、受理装置５２及び非受理装置５４に接続されている。

【００３０】

なお、他の検証者側装置６０は、上記検証者側装置４０と同様の構成であるため、詳細な説明を省略する。以下の説明では、検証者側装置４０を代表的な構成として、各部の名称を用いるものとする。

【００３１】

次に、本実施の形態のプロトコルを説明する。なお、システムパラメータは関数$F_g$、証明者の公開鍵はｖ＝Ｆ（ｇ，－ｓ）、証明者の秘密鍵はｓとする。

【００３２】

〔プロトコル〕

ステップ１：証明者は、

乱数発生器１４によって乱数ａを生成し、暗号演算器１８によって、Ａ＝Ｆ（ｇ，ａ）を計算し、通信Ｉ／Ｆ３０を介して暗号Ａを検証者に送信する。

このステップ１は、図１の証明者側装置１０の処理Ｐｓ１、及び処理Ｐｓ１の結果行われる通信Ｔ１に相当する。

【００３３】

ステップ２：検証者は、

乱数発生器４４によって乱数ｂを生成し、受信した暗号Ａを用いて、Ｂ＝Ｆ（ｇ

，ｂ）およびＸ＝Ｆ（Ａ，ｂ）を計算し、通信Ｉ／Ｆ３０を介して暗号Ｂ，Ｘを証明者に送信する。

このステップ２は、図１の検証者側装置４０が通信Ｔ１を受信した後の処理Ｑｓ１、及び処理Ｑｓ１の結果行われる通信Ｔ２に相当する。

【００３４】

ステップ３：証明者は、

受信した暗号Ｂ，Ｘを用いて、検証器２０により、Ｘ＝Ｆ（Ｂ，ａ）が成立するかを検査し、成立しなければ、検証者が不正を行っていると判断し、中断装置２４によりプロトコルを中断する。一方、成立するならば、乱数ｃを生成し、Ｃ＝Ｆ（ｇ，ｃ）、及びＹ＝Ｆ（Ｂ，ｃ）を計算する。なお、この計算は、Ｃ＝Ｆ（Ａ，ｃ）、Ｙ＝Ｆ（Ｘ，ｃ）でもよい。その後、Ｚ＝Ｈ（ａ，Ｙ，ｓ）すなわち、Ｚ＝ａ＋Ｙ＊ｓを計算し、計算結果であるＣ，Ｙ，Ｚを検証者に送信する。

このステップ３は、図１の証明者側装置１０が通信Ｔ２を受信した後の処理Ｐｓ２、及び処理Ｐｓ２の検証器２０による検証が成立した結果行われる通信Ｔ３に相当する。

【００３５】

ステップ４：検証者は、

受信した暗号Ｃ，Ｙ，Ｚを用いて、検証器５０により、Ｙ＝Ｆ（ｃ，ｂ）およびＡ＝Ｊ（ｖ，Ｙ，ｇ，Ｚ），すなわちＡ＝Ｆ（ｖ，Ｙ）＊Ｆ（ｇ，Ｚ）が成立するかを検査し、両方が成立すれば証明者の身元を受理する（受理装置５２が作動する）。一方、成立しないときは、証明者の身元を拒否する（非受理装置５４が作動する）。

このステップ４は、図１の検証者側装置４０が通信Ｔ３を受信した後の処理Ｑｓ２に相当する。

【００３６】

上記プロトコルは、証明者用及び検証者用の処理プログラムとして記録媒体としてのフロッピーディスクに実行可能な形式で格納することができる。この場合、各装置に挿抜可能なフロッピーディスクユニット（ＦＤＵ）を接続して、フロッピーディスクからＦＤＵを介して記録された処理プログラムを実行すればよい

。また、処理プログラムをコンピュータ内のＲＡＭや他の記憶領域（例えばハードディスク装置）にアクセス可能に格納にして（インストール）して実行するようにしてもよい。また、予めＲＯＭに記憶してもよい。また、記録媒体としては、ＣＤ－ＲＯＭ，ＭＤ，ＭＯ，ＤＶＤ等のディスクやＤＡＴ等の磁気テープがあり、これらを用いるときには、対応する装置としてＣＤ－ＲＯＭ装置、ＭＤ装置、ＭＯ装置、ＤＶＤ装置、ＤＡＴ装置等を用いればよい。

【００３７】

＜具体例＞

次に、上記プロトコルを用いたユーザ認証の具体例を説明する。なお、以下の具体例では、素数ｐ、ｑ（ただし、ｑ｜ｐ－１）と位数ｑの元ｇをシステムパラメータとしたときに、関数Ｆとして$v=F(g,-s)=g^{-s} \bmod p$を用いている。すなわち、鍵構成は、上述のSchnorrと同様のものを用いることができる。また、関数Ｈとして$H(a,Y,s)=a+Ys \bmod q$を用い、関数Ｊとして$J(v,Y,g,Z)=v^{Y}g^{Z} \bmod p$を用いている。

【００３８】

〔鍵構成〕

システムパラメータ：素数ｐ、ｑ（ただし、ｑ｜ｐ－１）と位数ｑの元ｇ

証明者の公開鍵：$v=g^{-s} \bmod p$

証明者の秘密鍵：$s \in Z_q$

【００３９】

〔プロトコル〕

ステップ１：証明者は、乱数ａを生成し、暗号Ａを計算し、検証者に送信する。

$$a \in Z_q \qquad \cdots (1)$$

$$A=g^{a} \bmod p \qquad \cdots (2)$$

すなわち、証明者側装置１０では、乱数発生器１４がシステムパラメータｑを用いて（１）式に基づく乱数ａを生成する。そして、暗号演算器１８は、その乱数ａ及びシステムパラメータｐ，ｇを用いて（２）式により暗号Ａを求める。この求めた暗号Ａは通信Ｉ／Ｆ３０に出力され、ネットワーク３２を介して検証者

側装置４０へ送信される。

【００４０】

ステップ２：検証者は、乱数ｂを生成し暗号ＢとＸを計算し証明者に送信する。

$$b \in Z_q \quad \cdots (3)$$

$$B = g^b \bmod p \quad \cdots (4)$$

$$X = A^b \bmod p \quad \cdots (5)$$

すなわち、検証者側装置４０では、通信Ｉ／Ｆ５６を介して暗号演算器４８に証明者側装置１０からの暗号Ａが入力される。このとき、検証者側装置４０では、乱数発生器４４がシステムパラメータｑを用いて（３）式に基づく乱数ｂを生成する。暗号演算器４８は、その乱数ｂ及び受信した暗号Ａを用いて（４）、（５）式により暗号Ｂと暗号Ｘを求める。この求めた暗号Ｂ，Ｘは通信Ｉ／Ｆ５６に出力され、ネットワーク３２を介して証明者側装置１０へ送信される。

【００４１】

ステップ３：証明者は、暗号Ｂ，Ｘを用い、次の（６）式が成立するかを検査し、成立しなければ、検証者が不正を行っていると判断し、プロトコルを中断する。一方、成立するならば、乱数ｃを生成し、暗号Ｃ、Ｙを求める。その後、暗号Ｚを求め、暗号Ｃ，Ｙ，Ｚを検証者に送信する。

$$X = B^a \bmod p \quad \cdots (6)$$

$$c \in Z_q \quad \cdots (7)$$

$$C = g^c \bmod p \quad \cdots (8)$$

$$Y = B^c \bmod p \quad \cdots (9)$$

$$\text{または} C = A^c \bmod p \quad \cdots (10)$$

$$Y = X^c \bmod p \quad \cdots (11)$$

$$Z = a + Ys \bmod q \quad \cdots (12)$$

すなわち、証明者側装置１０では、通信Ｉ／Ｆ３０を介して検証器２０に検証者側装置４０からの暗号Ｂ，Ｘが入力される。検証器２０は、暗号Ｂ，Ｘ及びメモリ１６に記憶したシステムパラメータを用いて上記（６）式に従って暗号Ｂ，Ｘを検証する。

検証器２０は、（６）式が非成立の検証結果である場合、中断装置２４へ信号

を出力し、プロトコルを中断させる。一方、（６）式が成立する検証結果の場合、検証器２０は、乱数発生器２２へ信号出力して、乱数発生器４４においてシステムパラメータｑに基づく乱数ｃを生成させる。この乱数ｃは、暗号演算器２６へ出力され、暗号演算器２６は、その乱数ｃ、受信した暗号Ｂ及びシステムパラメータ　　ｐ、ｇを用いて上記（８）、（９）式または（１０）、（１１）に従って暗号ＣとＹを求める。次に、求めた暗号Ｙ、乱数ａ、秘密鍵ｓ、システムパラメータｑを用いて（１２）に従って暗号Ｚを求める。これら求めた暗号Ｃ，Ｙ，Ｚは通信Ｉ／Ｆ３０に出力され、ネットワーク３２を介して検証者側装置４０へ送信される。

【００４２】

ステップ４：検証者は、次の（１２）、（１３）式が成立するかを検査し、両方が成立すれば証明者の身元を受理する。さもなくば、証明者の身元を拒否する。

$$Y = C^{b} \bmod p \qquad \cdots (13)$$

$$A = v^{Y} g^{Z} \bmod p \qquad \cdots (14)$$

すなわち、検証者側装置４０では、通信Ｉ／Ｆ５６を介して検証器５０に証明者側装置１０からの暗号Ｃ，Ｙ，Ｚが入力される。検証器５０は、暗号Ｃ，Ｙ，Ｚ及びメモリ４６に記憶したシステムパラメータを用いて上記（１３）式と、（１４）式に従って暗号Ｃ，Ｙ，Ｚを検証する。

検証器５０は、（１２）、（１３）式が非成立の検証結果である場合には、非受理装置５４を作動させ、証明者の身元を拒否する。一方、検証器５０は、上記式が成立する検証結果の場合には、受理装置５２を作動させ、証明者の身元を受理する。

【００４３】

本実施の形態では、証明者と検証者との間で、３回の通信のみでユーザ認証が可能である。そして、その通信量は、素数ｐ、ｑに寄与する。本実施の形態では、通信Ｔ１時に暗号Ａによる｜ｐ｜、通信Ｔ２時に暗号Ｂ，Ｘによる２｜ｐ｜、通信Ｔ３時に暗号Ｃ，Ｙ，Ｚによる２｜ｐ｜と｜ｑ｜である（図１参照）。このため、５｜ｐ｜＋｜ｑ｜のわずかな通信量でよいことになる。また、計算量については、上記各式から理解されるように、べき乗の演算負荷の寄与が大きい。こ

のべき乗の回数は、６回でよく、効率的なプロトコルとなることが理解されよう。

【００４４】

上記では、証明者と単一の検証者（一人の検証者）との間を例にして説明したが、インターネット等の非同期ネットワークにおいては、多数の検証者に対して証明者の身元確認が必要である。本実施の形態では、各検証者が通信Ｔ１～通信Ｔ３（図１参照）の間の何れの通信状態であっても、その途中の暗号Ａ，Ｂ，Ｃ，Ｘ，Ｙ，Ｚから秘匿すべき秘密鍵が傍受されるまたは解析されることはなく、秘匿性を維持することができる。このことは、以下で詳細に説明する。従って、多数の検証者に対して証明者が略同時や逐次に認証する場合でも、多数の検証者の各々に対して確実にユーザ認証することができる。これによって、インターネット等の非同期ネットワークを介して多数の検証者に対して証明者の身元を確認させるときに、安全にユーザ認証することができる。

【００４５】

なお、上記具体例は一方向性関数Ｆの具体例としてＺｐ上のべき乗演算を用いている。いわゆる、離散対数問題に基づく一方向性関数である。しかし、本発明はこれに限定されるものではない。このほかにも、Ｎを合成数としたとき、ＺＮ上の離散対数問題であってもよいし、また、楕円曲線上の離散対数問題であってもよい。

【００４６】

〔プロトコルの有効性〕

次に、本実施の形態のプロトコルの有効性を説明する。すなわち、本実施の形態のプロトコルが非同期ネットワークに適用された場合においても、零知識性を満たすことを、上記説明した＜具体例＞に基づいて説明する。なお、従来の技術の欄に説明したプロトコルでは、非同期ネットワークにおいて零知識性を満たさないことは、すでに知られている（C. Dwork, M. Naor and A. Shai, "Concurrent Zero-Knowledge, " Proc. Of 30th STOC, 1998）。

【００４７】

非同期ネットワークでは複数の結託する不正な検証者（Ｖ１，Ｖ２，・・・，

Ｖｎ）は同時に、証明者Ｐと通信することが可能である。従って、証明者Ｐと単一の検証者Ｖとの通信を考えるだけでは不十分である。すなわち、証明者Ｐと複数の検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）との間の通信の零知識性を考える必要がある。

【００４８】

そこで、本検証では、複数の結託した不正な検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）が提案するプロトコルに従い証明者Ｐと通信することによって得ることができる情報は、証明者Ｐと通信しなくても、得ることができることを証明する。具体的には、任意の不正な検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）に対して、あるアルゴリズムＳ（シミュレータ）が存在し、Ｓの出力が、実際の証明者Ｐと検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）の通信内容の確率分布と一致することを示す。ここでは、「アルゴリズムＳは実際の証明者Ｐと検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）の通信内容をシミュレートする」と表現する。

【００４９】

〔検証者の結託〕

一般性を失うことなく、不正な検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）は結託し、以下のように証明者Ｐと通信すると想定してよい。検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）を検証者（Ｇ１，Ｇ２，・・・，Ｇｍ）にグループ分けする（ｍ＜＝ｎ）。直観的には、グループ$G_i$に属する検証者は、グループ$G_{i-1}$に属する検証者の得た情報に基づいて、証明者Ｐと通信することを想定している。

【００５０】

〔一般化された結託プロトコル〕

入力を証明者Ｐの公開鍵およびシステムパラメータ（ｐ，ｑ，ｇ，ｖ）とする。

【００５１】

ステップ１：証明者Ｐは、暗号$A1 = g^{a1}$，$A2 = g^{a2}$，・・・，$An = g^{an}$ ｍｏｄ ｐを計算し、暗号（Ａ１，Ａ２，・・・，Ａｎ）を、それぞれ、検証者（Ｖ１，Ｖ２，・・・，Ｖｎ）に送信する。

この時点で検証者が得る情報は、$VIEW_0$＝｛（ｐ，ｑ，ｇ，ｖ），（Ａ１，Ａ２，・・・，Ａｎ）｝である。

【００５２】

ステップ２－１－Ｐ：Ｇ１に属するすべての検証者Ｖｉは、受信した暗号（Ａ１，Ａ２，・・・，Ａｎ）から、乱数ｂｉ∈$Z_q$を生成し、暗号Ｂｉ（＝$g^{bi}$ ｍｏｄ ｐ）および暗号Ｘｉ（＝$Ai^{bi}$ ｍｏｄ ｐ）を計算し、得られた暗号（Ｂｉ，Ｘｉ）を証明者Ｐに送信する。

【００５３】

ステップ２－１－Ｖ：Ｖｉ∈Ｇｉを満たす各ｉについて、証明者Ｐは検証式（Ｘｉ＝$B^{ai}$ ｍｏｄ ｐ）が成り立つか否かを検証する。

もし成り立てば、検証者Ｖｉに、暗号（Ｃｉ，Ｙｉ，Ｚｉ）を送信する。

この時点で、検証者が得る情報は、$VIEW_1=VIEW_0 \cup \{(Bi, Xi, Ci, Yi, Zi) \mid Vi \in G1\}$である。

【００５４】

次に、２＜＝ｋ＜＝ｎに対して、ステップ２－ｋ－Ｐ，２－ｋ－Ｖを繰り返して処理する。

【００５５】

ステップ２－ｋ－Ｐ：Ｇｋに属するすべての検証者Ｖｉは、これまでに得た情報$VIEW_{k-1}$から、乱数ｂｉ（∈Ｚｑ）、を生成し、暗号Ｂｉ（＝$g^{bi}$ ｍｏｄ ｐ）及び暗号Ｘｉ（＝$Ai^{bi}$ ｍｏｄ ｐ）を計算し、得られた暗号（Ｂｉ，Ｘｉ）を証明者Ｐに送信する。

【００５６】

ステップ２－ｋ－Ｖ：Ｖｉ∈Ｇｋを満たす各ｉについて、証明者Ｐは検証式（Ｘｉ＝$B^{ai}$ ｍｏｄ ｐ）が成り立つか否かを検証する。

もし成り立てば、検証者Ｖｉに、暗号（Ｃｉ，Ｙｉ，Ｚｉ）を送信する。

この時点で、検証者が得る情報は、$VIEW_k=VIEW_{k-1} \cup \{(Bi, Xi, Ci, Yi, Zi) \mid Vi \in Gk\}$である。

【００５７】

以上のことから最終的に結託する検証者が得る情報は

ＶＩＥＷｎ＝｛（ｐ，ｑ，ｇ，ｖ），

（Ａ１，Ａ２，・・・，Ａｎ），

（Ｂ１，Ｂ２，・・・，Ｂｎ），
（Ｘ１，Ｘ２，・・・，Ｘｎ），
（Ｃ１，Ｃ２，・・・，Ｃｎ），
（Ｙ１，Ｙ２，・・・，Ｙｎ），
（Ｚ１，Ｚ２，・・・，Ｚｎ）｝

である。

【００５８】

〔結託における計算量的仮定〕

上記ステップ２－ｋ－Ｖにおいて、各ｉに対して、

$Xi = B^{ai} \bmod p$

が成り立つためには、検証者Ｖｉは何らかの乱数ｂｉ ∈ Ｚｑを使って、

$Bi = g^{bi} \bmod p$ および $Xi = Ai^{bi} \bmod p$

を計算しなければならない。つまり、各検証者Ｖｉは乱数ｂｉの値を知っていると仮定する。この仮定は、形式的には以下のように述べることができる。

【００５９】

〔b-awareness assumption：以下ＢＡＡ〕

任意の検証者Ｖｉに対して、上記ステップ２－１－Ｖ，２－２－Ｖ，・・・，２－ｎ－Ｖにおいて、暗号（Ｂｉ，Ｘｉ）の値だけではなく、乱数ｂｉの値も出力するような、別の検証者Ｖｉ’が存在するとする。

【００６０】

〔シミュレーターの構成〕

以下のようにシミュレータＳを構成することにより、ＢＡＡの下で、零知識性を証明することができる。シミュレータＳは検証者（Ｖ１’，Ｖ２’，・・・，Ｖｎ’）をサブルーチンとして利用する。これにより、シミュレータＳは各乱数ｂｉの値を利用することができる。

【００６１】

〔シミュレーターのアルゴリズム〕

入力：公開鍵ｖ，システムパラメータｐ，ｑ，ｇ

出力：$VIEW_n$＝｛（ｐ，ｑ，ｇ，ｖ），

（Ａ１，Ａ２，・・・，Ａｎ），
（Ｂ１，Ｂ２，・・・，Ｂｎ），
（Ｘ１，Ｘ２，・・・，Ｘｎ），
（Ｃ１，Ｃ２，・・・，Ｃｎ），
（Ｙ１，Ｙ２，・・・，Ｙｎ），
（Ｚ１，Ｚ２，・・・，Ｚｎ）｝

【００６２】

ステップ１：全てのｉ（１＜＝ｉ＜＝ｎ）について、乱数Ｙｉ ∈ $Z_q$，Ｚｉ ∈ $Z_q$を生成し、Ａｉ＝$V^{Yi} g^{Zi}$を計算する。この時点でＳがシミュレートした情報は、

$View_0$＝[(ｐ，ｑ，ｇ，ｖ)，(Ａ１，Ａ２，・・・，Ａｎ)]

である。

ステップ２－１－Ｐ：Ｇ１に属するすべての検証者Ｖｉ（Ｖｉ’）を実行する。つまり、各ＶｉにＶＩＥ$W_0$を入力し、（Ｂｉ，Ｘｉ，ｂｉ）を計算する。このとき、Ｂｉ＝$g^{bi}$ ｍｏｄ ｐが成り立つ。

ステップ２－１－Ｖ：Ｙｉ＝$Ci^{bi}$ ｍｏｄ ｐを満たすＣｉを計算する。この時点で、シミュレータＳがシミュレートした情報は、$VIEW_1$＝$VIEW_0$ ∪ ｛（Ｂｉ，Ｘｉ，Ｃｉ，Ｙｉ，Ｚｉ）｜Ｖｉ∈Ｇ１｝である。

【００６３】

２＜＝ｋ＜＝ｎに対して、ステップ２－ｋ－Ｐ，２－ｋ－Ｖを繰り返す。

【００６４】

ステップ２－ｋ－Ｐ：Ｇｋに属するすべての検証者Ｖｉ（Ｖｉ’）を実行する。つまり、各Ｖｉに$VIEW_{k-1}$を入力し、（Ｂｉ，Ｘｉ，ｂｉ）を計算する。このとき、Ｂｉ＝$g^{bi}$ ｍｏｄ ｐが成り立つ。

ステップ２－ｋ－Ｖ：Ｙｉ＝$Ci^{bi}$ ｍｏｄ ｐを満たすＣｉを計算する。この時点で、Ｓがシミュレートした情報は、$VIEW_k$＝$VIEW_{k-1}$ ∪ ｛（Ｂｉ，Ｘｉ，Ｃｉ，Ｙｉ，Ｚｉ）｜Ｖｉ∈$G_k$｝である

【００６５】

最終的にシミュレートされる通信内容ＶＩＥＷ$_n$は、実際の証明者Ｐと（Ｖ１，Ｖ２，・・・，Ｖｎ）の通信内容の確立分布と一致する。従って、零知識性が満たされることになる。

【００６６】

【発明の効果】

以上説明したように本発明によれば、証明者側装置と検証者側装置との間で授受される情報から、証明者側装置の秘密鍵が漏洩することがなく、確実にユーザ認証が行える、という効果がある。

特に、インターネットなどの非同期ネットワークを介して、証明者側装置が複数の検証と同時に認証に必要な情報を授受した場合でも、零知識性が満たされるので、そのようなネットワークを介しても、証明者側装置の秘密鍵が漏洩することはなく、確実にユーザ認証を行うことができる、という効果がある。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係るプロトコルを示すフローチャートである。

【図２】

本発明の実施の形態に係る証明者側装置と検証者側装置との概略構成を示すブロック図である。

【図３】

従来のプロトコルを示すフローチャートである。

【図４】

証明者と検証者とが１対１で通信することを説明するための説明図である。

【図５】

証明者と検証者とが１対多で通信することを説明するための説明図である。

【符号の説明】

１０　証明者側装置

１２　入力装置

１４　乱数発生器

１６　メモリ

１８　暗号演算器

２０　検証器

２２　乱数発生器

２４　中断装置

２６　暗号演算器

２８　暗号演算器

３２　ネットワーク

４０　検証者側装置

４２　入力装置

４４　乱数発生器

４６　メモリ

４８　暗号演算器

５０　検証器

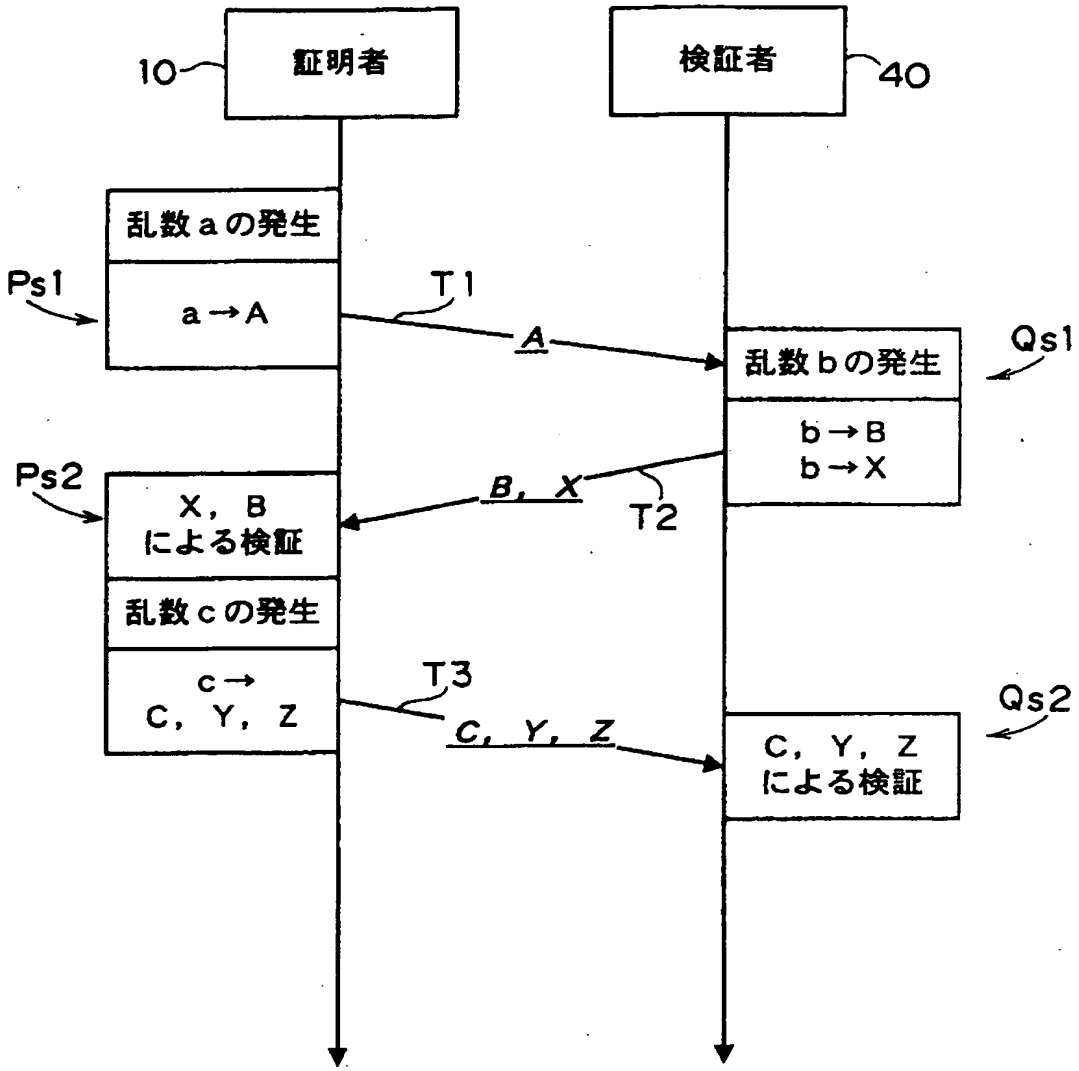
５２　受理装置

５４　非受理装置

６０　検証者側装置

【書類名】　　図面

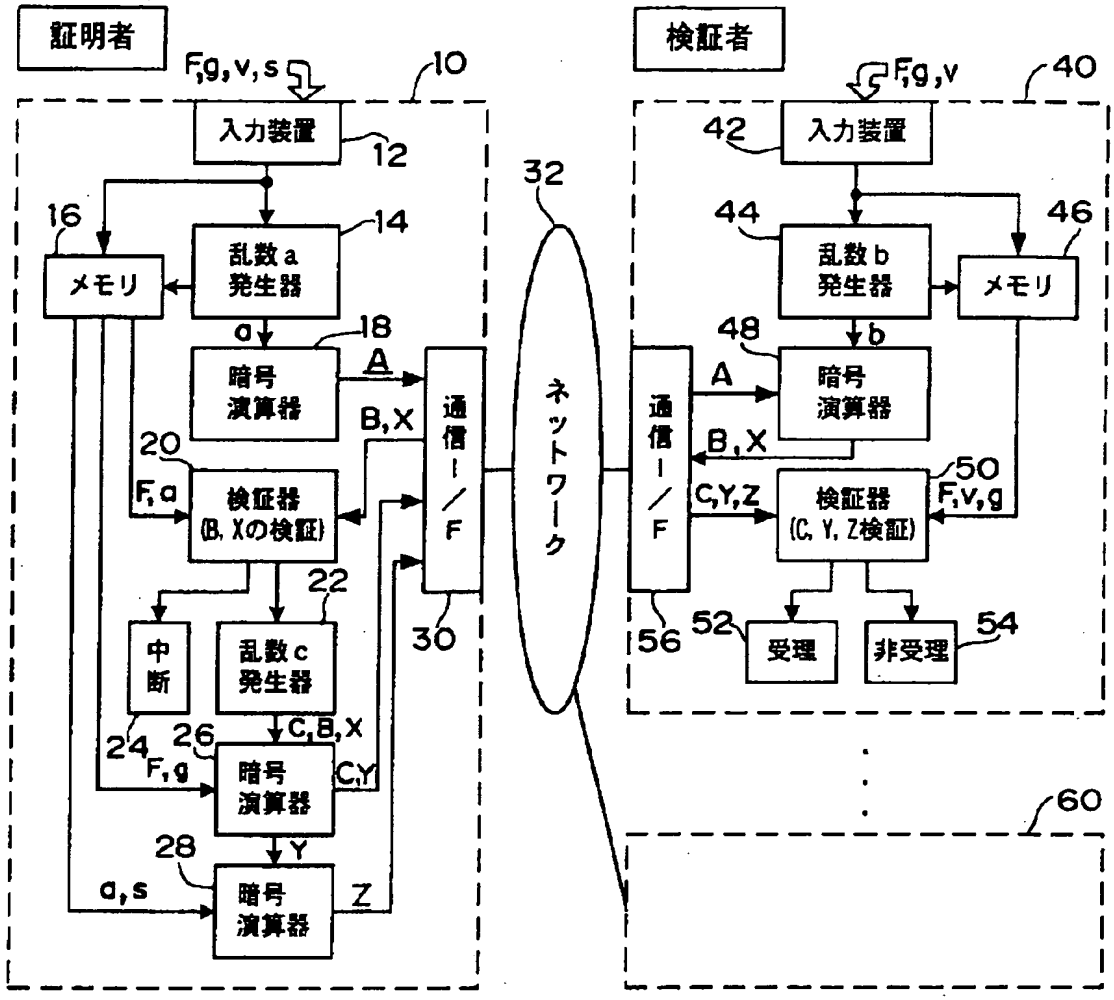
【図１】



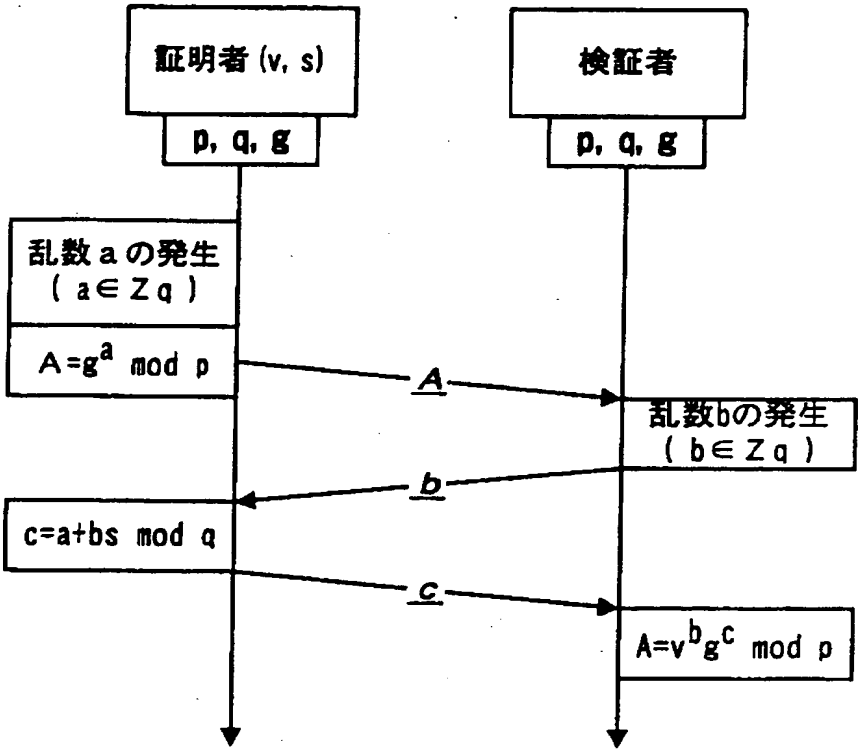



出証特２０００－３０７４７６８

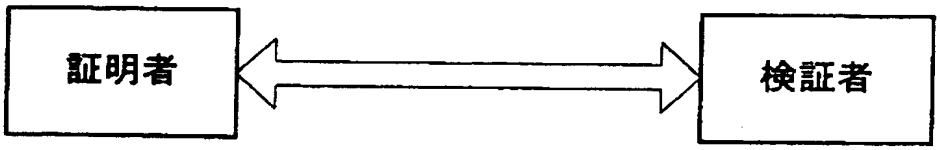
【図２】


証明者
検証者
F,g,v,s
F,g,v
10
40
入力装置
12
42
入力装置
32
16
14
44
46
乱数a
発生器
メモリ
乱数b
発生器
メモリ
a
18
48
b
A
暗号
演算器
A
暗号
演算器
B,X
通信
I/
F
ネットワーク
通信
I/
F
B,X
20
50
F,a
検証器
(B, Xの検証)
C,Y,Z
検証器
(C, Y, Z検証)
F,v,g
22
中
断
乱数c
発生器
30
56
52
受理
非受理
54
24
26
C,B,X
F,g
暗号
演算器
C,Y
60
28
Y
a,s
暗号
演算器
Z

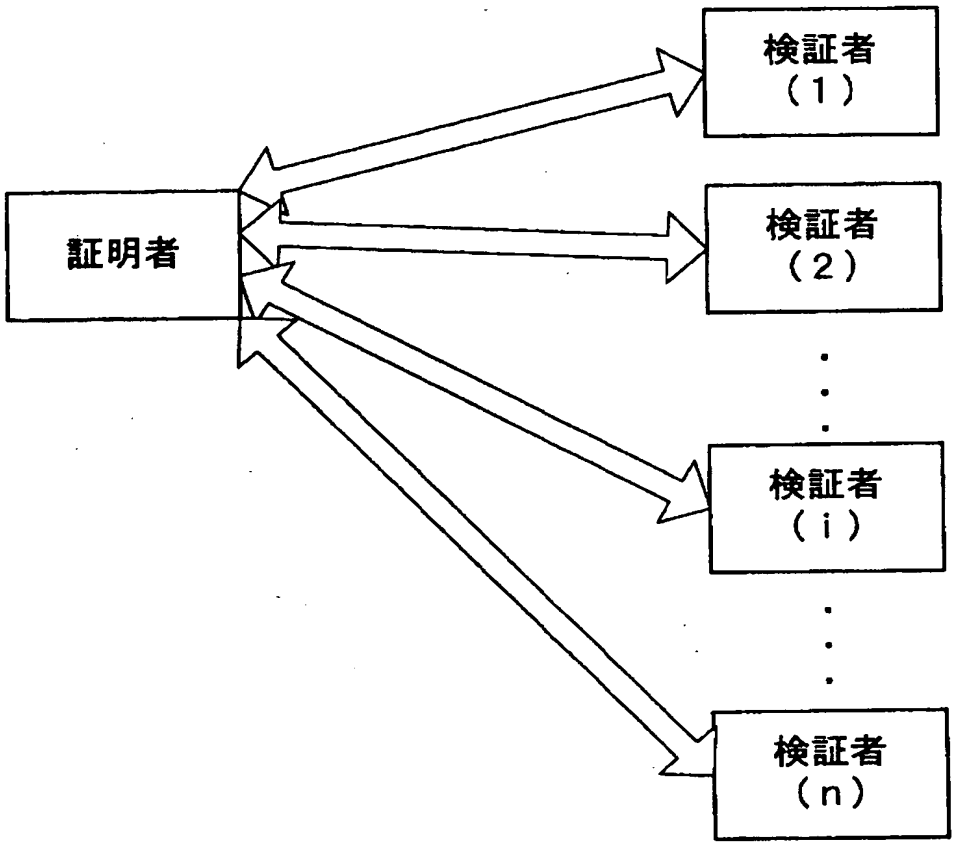
【図３】


証明者 (v, s)
p, q, g
検証者
p, q, g
乱数ａの発生
( a∈Zq )
A=g^a mod p
A
乱数bの発生
( b∈Zq )
b
c=a+bs mod q
c
A=v^b g^c mod p

【図４】


証明者
検証者

【図５】



【書類名】　　要約書

【要約】

【課題】　証明者と検証者が多数の場合であっても零知識性を満たしながら安全にユーザ認証する。

【解決手段】　プロトコルのステップ１で、証明者１０は、乱数ａによるＡ＝Ｆ（ｇ，ａ）を計算して検証者に送信する（処理Ｐｓ１、通信Ｔ１）。ステップ２で、検証者４０は、乱数ｂによる暗号Ｂ＝Ｆ（ｇ，ｂ）、Ｘ＝Ｆ（Ａ，ｂ）を計算して証明者に送信する（処理Ｑｓ１、通信Ｔ２）。ステップ３で、証明者は、Ｘ＝Ｆ（Ｂ，ａ）が成立性を検査し、非成立ならばプロトコルを中断し、成立ならば、乱数ｃによるＣ＝Ｆ（ｇ，ｃ）、Ｙ＝Ｆ（Ｂ，ｃ）を計算した後、Ｚ＝Ｈ（ａ，Ｙ，ｓ）を計算し、検証者に送信する（処理Ｐｓ２、通信Ｔ３）。ステップ４で、検証者は、Ｙ＝Ｆ（Ｃ，ｂ）およびＡ＝Ｊ（ｖ，Ｙ，ｇ，Ｚ）が成立性を検査し、成立ならば証明者の身元を受理し、非成立ならば証明者の身元を拒否する（処理Ｑｓ２）。

【選択図】　　図１

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２０００－０９９８６７ |
| 受付番号 | ５００００４１２６５８ |
| 書類名 | 特許願 |
| 担当官 | 高田　良彦　　２３１９ |
| 作成日 | 平成１２年　5月３１日 |

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 390009531
- 【住所又は居所】 アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
- 【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【復代理人】 申請人
- 【識別番号】 100079049
- 【住所又は居所】 東京都新宿区新宿４丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
- 【氏名又は名称】 中島　淳

【選任した復代理人】
- 【識別番号】 100084995
- 【住所又は居所】 東京都新宿区新宿４丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
- 【氏名又は名称】 加藤　和詳

【選任した復代理人】
- 【識別番号】 100085279

次頁有

# 認定・付加情報（続き）

【住所又は居所】　東京都新宿区新宿四丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
【氏名又は名称】　西元　勝一
【選任した復代理人】
【識別番号】　100099025
【住所又は居所】　東京都新宿区新宿４丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
【氏名又は名称】　福田　浩志

次頁無

# 出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　１９９０年１０月２４日
［変更理由］　新規登録
住　所　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　インターナショナル・ビジネス・マシーンズ・コーポレイション

２．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　インターナショナル・ビジネス・マシーンズ・コーポレーション